TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/05/2020

SUBJECT:
A Vulnerability in F5 BIG-IP Traffic Management User Interface Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in F5 BIG-IP Traffic Management User Interface (TMUI), which could allow for remote code execution. F5's BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions. Successful exploitation of this vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the TMUI, through the BIG-IP management port and/or Self IPs, to execute remote system commands, create or delete files, disable services, and/or execute remote Java code. This vulnerability may result in complete system compromise.

THREAT INTELLIGENCE:
This vulnerability has been reported being actively exploited in the wild and a PoC scanner is available on Github.

SYSTEMS AFFECTED:

1. F5 BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) 15.x versions prior to 15.1.0.4
2. F5 BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) 14.x versions prior to 14.1.2.6
3. F5 BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) 13.x versions prior to 13.1.3.4
4. F5 BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) 12.x versions prior to 12.1.5.2
5. F5 BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) 11.x versions prior to 11.6.5.2

RISK:
Government:

1. Large and medium government entities: **High**
2. Small government entities: **High**

Businesses:

1. Large and medium business entities: **High**

2. Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in F5 BIG-IP Traffic Management User Interface (TMUI), which could allow for remote code execution. This vulnerability can be exploited by sending a crafted HTTP request to the server hosting the Traffic Management User Interface (TMUI) utility for BIG-IP configuration. This vulnerability exists in undisclosed pages of the Traffic Management User Interface. (CVE-2020-5902).

Successful exploitation of this vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the TMUI, through the BIG-IP management port and/or Self IPs, to execute remote system commands, create or delete files, disable services, and/or execute remote Java code. This vulnerability may result in complete system compromise.

RECOMMENDATIONS:
The following actions should be taken:

1. Apply appropriate patches or appropriate mitigations provided by F5 to vulnerable systems immediately after appropriate testing.
2. Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
3. Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
4. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
5. Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
F5:
https://support.f5.com/csp/article/K52145254?sf235665517

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902

GitHub:
https://github.com/aqhmal/CVE-2020-5902-Scanner/